

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE

Strasbourg, 6 September 2016

CODEXTER (2016) 17

COMMITTEE OF EXPERTS ON TERRORISM (CODEXTER)

**COMPILATION OF CDPC OBSERVATIONS
ON DRAFT RECOMMENDATION REC(2005) 10**

Secretariat of the Counter-Terrorism Division

Information Society and Action against Crime Directorate, DG I

codexter@coe.int - www.coe.int/terrorism

COMPILATION OF CDPC OBSERVATIONS ON DRAFT RECOMMENDATION REC(2005) 10

On Friday 1 July 2016, the Secretariat asked the members of the European Committee on Crime Problems (CDPC) to submit possible comments/remarks/written proposals for amendments to the draft Recommendation Rec (2005) 10 of the Committee of Ministers to member States on special investigation techniques in relation to serious crimes including acts of terrorism.

What follows is a compilation of the comments and drafted suggestions sent by the representatives of the following countries:

❖ FRANCE:

16. Recognising that the use of special investigation techniques is a vital tool for preventing, suppressing and prosecuting the commission of the most serious crimes, including acts of terrorism;

Comment as regards France: attention needs to be paid to the scope of the Recommendation by limiting it, right from the preamble, to the judicial sphere alone and by making it clear that it does not apply to special investigation techniques used for the collection, exploitation and/or provision of information to national executive bodies for the purpose of preventing threats and risks liable to affect the life and security of the nation. In those circumstances, the use of special investigation techniques is subject to specific rules which cannot be affected by the present Recommendation.

Appendix

1. For the purpose of this Recommendation, “special investigation techniques” means techniques applied by the competent authorities in the context of criminal investigations for the purpose of ~~detecting and~~ investigating serious crimes and suspects, aiming at gathering information in such a way as not to alert the target persons.

2. For the purpose of this Recommendation, “competent authorities” means judicial, ~~prosecuting and investigating~~ authorities ~~involved in deciding, supervising or using~~ responsible for ordering and supervising the use of special investigation techniques in the context of criminal investigations in accordance with national legislation.

4. For the purpose of this Recommendation “cyber investigation” means a ~~an~~ criminal inquiry aimed at preventing, prosecuting and suppressing any serious crimes including acts of terrorism, as well as any criminal offence established by the Council of Europe Convention on the Prevention of Terrorism (CETS No. 196) and its additional Protocol (CETS No. 217) committed through the Internet and any unlawful interference with information, computer systems, computer programs, and data, that is committed intentionally for the purpose of any serious crimes including acts of terrorism.

7. Member states should take appropriate legislative measures to ensure adequate periodical review of the implementation of special investigation techniques by judicial authorities through prior authorisation, supervision during the investigation or ex post facto review.

Comment as regards France: this provision is acceptable only if the special investigation techniques referred to in this Recommendation are confined to special investigation techniques used in the context of a criminal investigation (and do not include special investigation techniques used for information purposes).

10. Member states should ensure proportionality between the special investigation techniques used and the legitimate aims pursued. In this respect, when deciding on their use, an evaluation in the light of the seriousness of the offence, the intrusive nature of the specific special investigation technique used, and the general complexity of the facts and urgency of such cases and the number of individuals involved should be made.

Comment as regards France: we do not feel that the number of individuals involved and urgency are appropriate criteria for evaluating the legitimacy of a special investigation technique.

~~11. Member states should ensure that competent authorities apply less intrusive investigation methods than special investigation techniques if such methods enable the offence to be detected, prevented or prosecuted with adequate effectiveness.~~

COMPILATION OF CDPC OBSERVATIONS ON DRAFT RECOMMENDATION REC(2005) 10

12-11. Member states should take appropriate legislative measures to permit the production of evidence gained from the lawful use of special investigation techniques before courts. Procedural rules governing the production and admissibility of such evidence shall safeguard the rights of the accused to a fair trial.

Comment as regards France: this provision is acceptable for France only if the Recommendation applies solely to special investigation techniques ordered in the context of a criminal investigation (and not to special investigation techniques used for information purposes)

14.13. Member states should ensure that, with respect to those special investigation techniques involving technical equipment, laws and procedures take account of the new technologies. ~~For this purpose, they should work closely with the private sector to obtain their assistance in order to ensure the most effective use of existing technologies used in special investigation techniques and to maintain effectiveness in the use of new technologies.~~

15. Member States should make appropriate and expeditious use of asset investigations ~~financial investigation techniques~~ with a view to disrupting the activities of criminal and terrorist associations or groups; depriving individuals, associations and groups of ~~all~~ assets; identifying and confiscating property that is or may be gathered by them for the purpose of committing serious crimes including acts of terrorism as well as any criminal offence established by the Council of Europe Convention on the Prevention of Terrorism (CETS No. 196) and its Additional Protocol (CETS No. 217).

17. Member States should facilitate the appropriate use of cyber investigations in order to prevent and suppress the perpetration of cyber-attacks for serious crimes including acts of terrorism, including those criminalised under the Council of Europe Convention on the Prevention of Terrorism (CETS No. 196) and its Additional Protocol (CETS No. 217).

20. Member states should ensure adequate training of competent authorities in charge of deciding to use, supervising and using special investigation techniques including financial and cyber investigations. Such training should comprise training on technical and operational aspects of special investigation techniques, training on criminal procedural legislation in connection with them and relevant training in human rights.

21. Member states should consider the provision of specialised advice at national level with a view to assisting or advising competent authorities in the use of special investigation techniques.

Comment as regards France: we are concerned about the relevance of these provisions: special investigation techniques are governed by specific provisions which form an integral part of criminal procedure. In principle, they are ordered and supervised by judicial authorities (prosecutors and judges) trained in criminal procedure. They are at the very heart of their work. Likewise, we cannot see what "relevant training in human rights" would mean here.

22. Member states should make use to the greatest extent possible of existing arrangements for judicial or police cooperation in relation to the use of special investigation techniques including financial and cyber investigations at both a national and international level. Where appropriate member states should also identify and develop additional arrangements to enhance cooperation on the fight against serious crimes including acts of terrorism, ~~paying particular attention to questions concerning jurisdiction in connection with the application of special investigation techniques on the internet including with the private sector.~~ *Comment as regards France: we do not understand this last point.*

23. Member states are encouraged to sign, to ratify and to implement existing conventions or instruments in the field of international cooperation in criminal matters in areas such as exchange of information, financial investigations, cyber investigations, ~~controlled delivery, covert investigations,~~ joint investigation teams, and cross-border operations. ~~and training.~~

❖ **DENMARK:**

The Danish delegation did not submit comments to the draft. However, the representative clarified: “We have understood the use of the expression *suppressing or suppress* in the text (in particular in pr. 4 and 17 in the appendix) as also covering investigations where a crime has already been committed.”

❖ **LATVIA:**

The draft recommendation Chapter II a. section (General Principles) Paragraph 7 states that the Member States should take appropriate legislative measure to ensure adequate periodical review of the implementation of special investigation techniques by judicial authorities through prior authorization, supervision during the investigation or ex post facto review. Common terminology should be used throughout the draft recommendation, consequently, the term "judicial authorities" should be replaced by the term "competent authorities" – as used in the draft recommendation Chapter I (Definitions and scope) paragraph 2.

❖ **SLOVENIA:**

To: CDPC

We would like to invite CODEXTER to consider:

- limiting the scope of the amended Recommendation to the covert (special investigative) techniques within financial (cyber) investigation, in the context of criminal investigation;
- the coherence of the potential expansion of the scope of Recommendation also to the non-criminal procedural measures (techniques) within the financial investigation (such as administrative measures by FIU – see paragraph 15);
- focusing the scope of the Recommendation to the covert (special investigation) techniques within the financial/cyber investigation, rather than the broader reference to the financial/cyber investigation.

To: CODEXTER

Further to our comments from 10.6.2016 to the Drafting group (prior to their meeting on 13-14.6.2016) we would like to emphasize that we support highlighting the relevance of tracing, freezing and confiscation of proceeds of crime by “financial investigation” as an important and integrative part of the criminal investigation of profit generating criminal offences.

We would like to invite CODEXTER to consider limiting the scope of the amended Recommendation to the covert (special investigative) techniques within financial (cyber) investigation, in the context of criminal investigation.

The Recommendation applies to the special investigation techniques within criminal investigation/procedure (Chapter I, paragraph 1). Only some financial investigation techniques (such as bank account monitoring) correspond to the SIT definition, while the FI can be described as a wider process (similar or parallel to criminal investigation) within, or related, to criminal investigation (criminal or in rem confiscation, preventive (administrative?) measures, such as temporal freezing by FIU). (See paragraph 3 and distinction in paragraphs 15 and 16 .)

In our opinion widening the scope of the Recommendation to the techniques that are not “covert” and not “in the context of criminal investigation” could have contra productive effect.

We propose the following amendments to the draft proposal:

Add a new sentence at the end of paragraph 3:

This Recommendation applies also when special investigation techniques are used within or for the purpose of financial investigation.

Add a new sentence at the end of paragraph 4:

This Recommendation applies also when special investigation techniques are used within or for the purpose of cyber investigation.

Add: ... preventing, suppressing and investigating... in second line.

Delete paragraph 15 or further explain the purpose of distinction between paragraphs 15 and 16. What is the meaning of “depriving of all assets”?

Add in Paragraph 16: MS should facilitate the appropriate use of special investigation techniques within financial investigation, when inquiries are being made by the ~~proper~~ competent law enforcement agencies...

Mutatis mutandis in Paragraph 17: MS should facilitate the appropriate use of special investigation techniques within cyber investigation in order to prevent, investigate and suppress the perpetration...

Paragraph 20: ... special investigation techniques including within financial and cyber investigation...

Paragraph 22: ... special investigation techniques including within financial and cyber investigation...

❖ **SWITZERLAND:**

17. Aware that the use of special investigation techniques in criminal investigations requires confidentiality and that any efforts to pursue the commission of serious crime, including acts of terrorism, should ~~where appropriate~~ be thwarted where appropriate with secured covert means of operation;

Appendix

1. For the purpose of this Recommendation, “special investigation techniques” means techniques applied by the competent authorities in the context of criminal investigations for the purpose of detecting and investigating serious crimes ~~and suspects~~, aiming at gathering information in such a way as not to alert the target persons.

8. Member states should ensure that an individual or legal person who claims to be the victim of a breach of his rights occasioned by the misuse of special investigation techniques shall have the right of access to an effective remedy before a ~~national~~ designated authority.

19. Member states should take appropriate measures to ensure that the technology required for special investigation techniques, in particular with respect to interception of communications, meets ~~minimum~~ the requirements of confidentiality, integrity and availability.